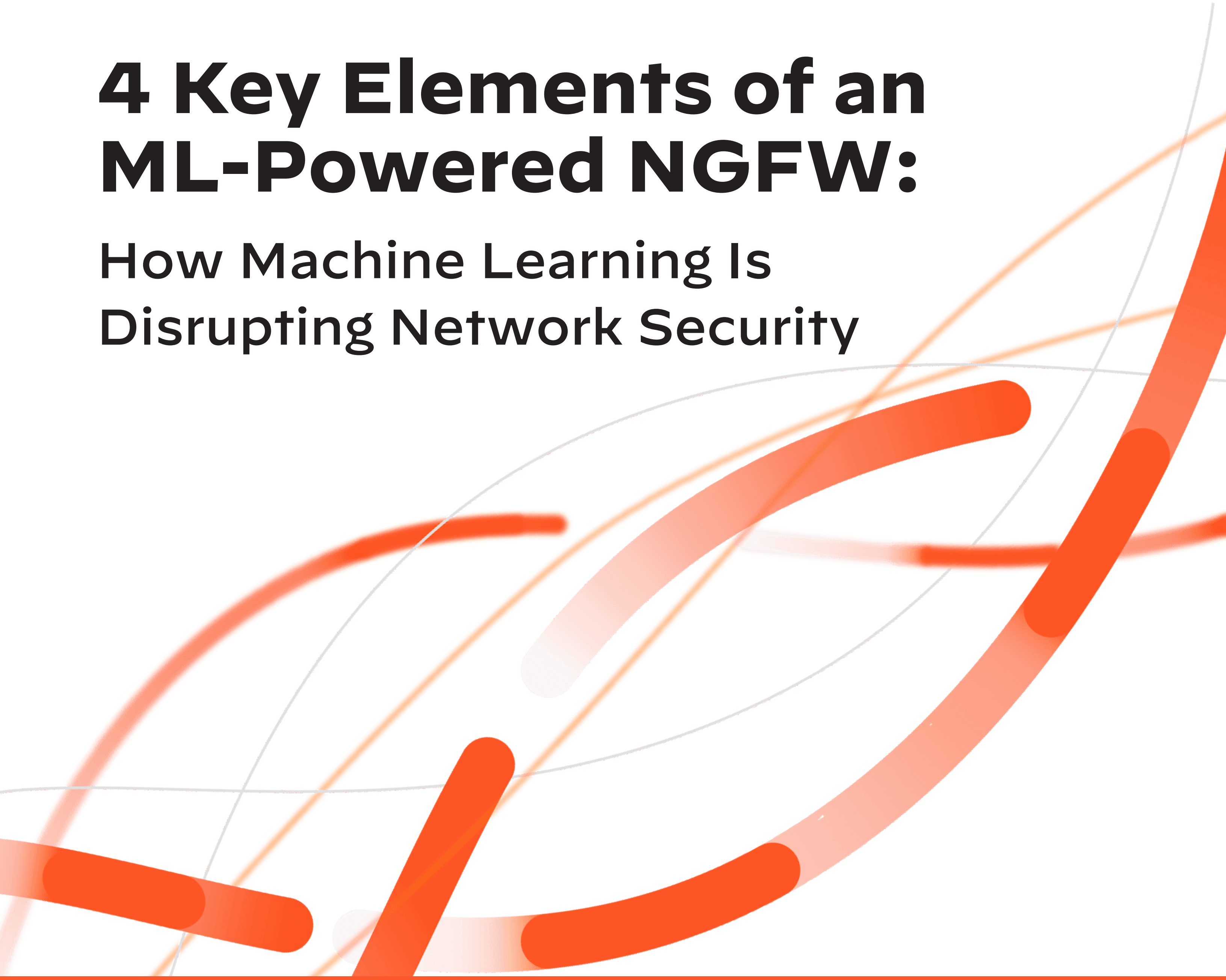
paloalto NETWORKS

# 4 Key Elements of an ML-Powered NGFW:

## How Machine Learning Is Disrupting Network Security



It's no secret that automation is being leveraged in virtually every business sector, with the core goal to drive efficiency and scale into systems. In the context of cybersecurity, automated data collection and processing plays a key role in protecting against data breaches and cyberattacks. However, adversaries can enjoy the same level of benefits of automation, using the techniques to help conduct malicious campaigns and make it easier for them to scale up their operations.

As an example of this paradox, consider the ongoing battle—or cat and mouse game—that typifies malware prevention. Over the last 10 years, the network security industry has focused on reducing the time it takes to react to new attacks. As an example, we've seen the time required to analyze, create a signature, and update all network security systems with those protections has been reduced from weeks to days to hours, and in some cases, even to minutes. However, cybercriminals don't stay still. Attacks are growing more frequent, with more variants and more speed. Specifically, attackers are using automation to deliver more and more variants of malware because they know they have a high chance of success.

Aside from attackers constantly changing and advancing their techniques, enterprises are facing new technology adoption trends that are surfacing new challenges and environmental complexity. The biggest tectonic shift has been the movement to the cloud. According to recent data from Forrester Research, over 67% of their clients adopted public cloud, with 80% of those leveraging a hybrid environment across multiple public clouds and on-premises infrastructures. Adding to this move to cloud to support digital transformation efforts is the continual need to support an increasingly remote workforce, a trend that was exploding even before the COVID-19 pandemic.

Finally, the proliferation of devices that IT needs to support and secure continues. This is evident in the dramatic adoption and deployment of the Internet of Things (IoT), which has gone from being an interesting concept to infiltrating wide swaths of enterprise infrastructure. IoT devices are being used in healthcare, across manufacturing plants, and are rapidly spreading to other industries. According to Unit 42, Palo Alto Networks' global threat intelligence team, IoT presents unprecedented cybersecurity risks, for the reasons illustrated below:

Zero to Minimum Built-In Security

Browse Interface Vulnerabilities

Outdated Operating Systems

Failure to Adhere to Security Best Practices

**Forrester Research on Cloud Adoption in 2020**

| 67% | 80% |
|---|---|
| clients adopted public cloud | of those leveraging hybrid cloud |

– **Stephanie Balaouras**
VP & Research Director for Security, Forrester

**"45% of enterprises already have some sort of IoT deployment. Another 26% are planning a deployment in the next 12 months"**

– **Stephanie Balaouras**
VP & Research Director for Security, Forrester

By all measures, the constantly changing environment, deployment, and security risk trends are combining to create a perfect storm for security administrators. It simply isn't possible with current controls to stay ahead of automation services and tactics of today's threat actors. Administrators can't keep security policy changes up to date fast enough using manual methods, let alone get visibility into what manner of devices are connecting to their networks. It's time for security admins to fight attacker automation with a proactive and disproportionate response.

To address these challenges, a new disruptive approach is needed. Instead of continuing down the well-worn path of reactive responses that simply reduce the response time and marginally improve the management burden, network security needs to become truly proactive. The industry needs a new type of firewall that, for the first time, embeds ML directly in the core of the firewall to provide real-time inline device identification and inline signatureless attack prevention. The solution must leverage cloud-based ML processes to push zero-delay signatures as well as instructions back to the firewall to stop attacks and reconfigure policies. Data intensive ML processes must automatically compute and recommend policy changes to optimize security utilization and outcomes. At the foundation, this solution must be built on a complete next-generation firewall (NGFW) for high performance, app- and user-based enterprise security. This is the era of the ML-Powered Firewall.

This e-book will help you to understand the four critical components of an ML-Powered NGFW to proactively prevent threats and see and secure the enterprise.

## What an ML-Powered NGFW Must Do

Given how the environment and threat landscape is changing, a revolutionary approach is needed. However, the solution needs to start with the NGFW as the foundation. The NGFW, deployed in physical, virtual, and cloud form factors and powered by cloud-delivered security services, remains the ideal control point in an enterprise, serving as the first line of defense in any solid security platform. NGFWs provide complete visibility across your network, as well as automated response capabilities to keep your organization safe. From this starting point, the NGFW needs to evolve to augment its existing automation capabilities with the power of ML—down to the core of its operations. In essence, an ML-powered NGFW can change the landscape. Instead of being reactive, it takes a proactive, cloud-based and ML-driven approach to keeping networks safe.

### An effective ML-powered NGFW must:

Deliver inline ML on the NGFW to prevent attacks, saving organizations from being the first victim in a cyberattack.

Be deployed consistently everywhere security is required, reducing gaps in visibility and controlling manual operational overhead.

Protect everything—users, data, devices, and all applications—not just popular or common ones.

# Four Essential Elements of an ML-Powered NGFW

To deliver these benefits, an ML-Powered NGFW needs four essential elements:

1. Inline ML-powered prevention on the NGFW
2. Zero-delay signatures leveraging massive cloud scale
3. ML-powered visibility across IoT and other connected devices
4. Automated, intelligent policy recommendations

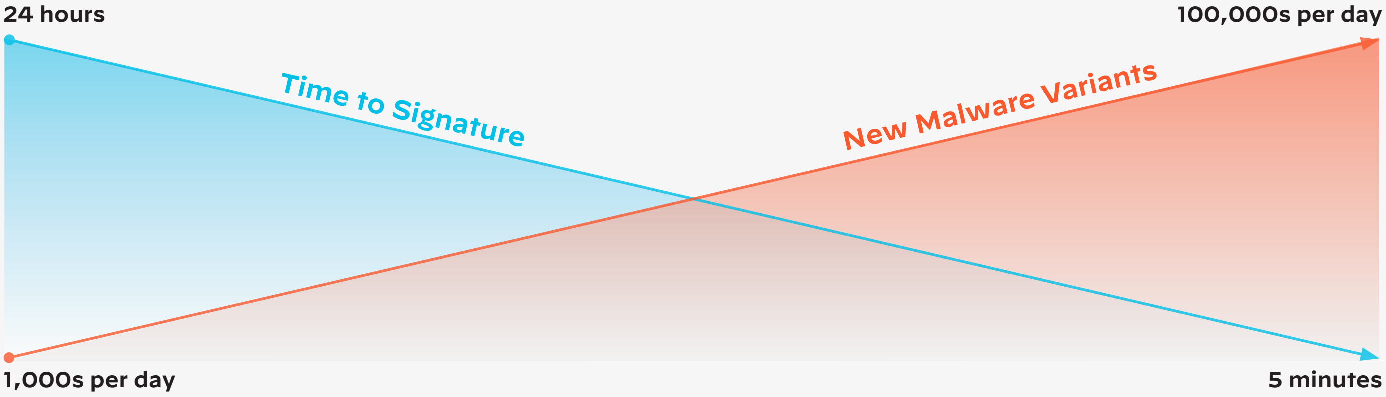
**Let's look at why these elements are important, how they work, and what benefits they deliver.**

## Inline ML-Powered Prevention on the NGFW

**Challenge:** Attackers increasingly leverage existing attacks and then modify them (in virtually all cases using automation) to bypass traditional signature-based security. While NGFWs are already able to detect variants of malware using heuristics, with polymorphic malware distributed at scale, often there is a first victim who falls prey to the attack before any security services can reprogram the infrastructure to prevent subsequent attacks. That first attack could often still be prevented at a later stage, but this adds risk and effort.

Adding more signatures or deploying them faster doesn't solve the issue, nor does collecting files and releasing them very slowly to the end user, thus being able to perform zero-day checks, such as sandboxing, on a file before it completely reaches the end user. Approaches such as these involve  stopping every file or website request for inspection and analysis until it is deemed benign. This method hasn't been very successful either. Holding files hinders business productivity, introduces operational complexity, and causes a poor user experience. Moreover, the approach simply doesn't scale. The more files sent for analysis, the more files are held and sidelined, and the more business must slow down.

Cat and Mouse Game—Faster Signatures Alone Won't Stop Attackers



**What an ML-Powered NGFW Does:** While firewalls have taken initial strides to incorporate ML, they have done so using half measures. For example, to avoid degrading performance on the firewall, other solutions deploy or integrate with offline malware analysis systems in parallel that leverage ML and then incorporate the results for enforcement. In contrast, an ML-Powered NGFW embeds ML algorithms directly within the core of the firewall, making classification decisions at "line speed." This means that the ML-Powered NGFW can find malware in real time, inspecting a file while it's being downloaded and blocking malicious files before they can complete. This instant blocking occurs, in other words, while content is streaming through the firewall, maintaining the leading performance requirements and enabling a single pass inspection. As a result, with inline prevention, the ML-Powered NGFW automatically prevents initial infections from never-before-seen threats without requiring cloud-based or offline analysis for the majority of malware variant threats, reducing the time between visibility and prevention to near zero.

Inline ML-powered prevention on the NGFW helps prevent the most challenging and prevalent threats, including portable executables, phishing, malicious JavaScript, and fileless attacks. The models are tuned to avoid false positives, and the system includes a unique feedback loop that ensures ongoing accuracy.

## Scenario: Phishing Webpage to Steal Credentials

**Situation:** As part of a targeted attack designed to steal credentials, an attacker crafts and hosts a phishing webpage, potentially with malicious content within custom domains, compromised legitimate websites, or in some cases, webpages only visible to the target.

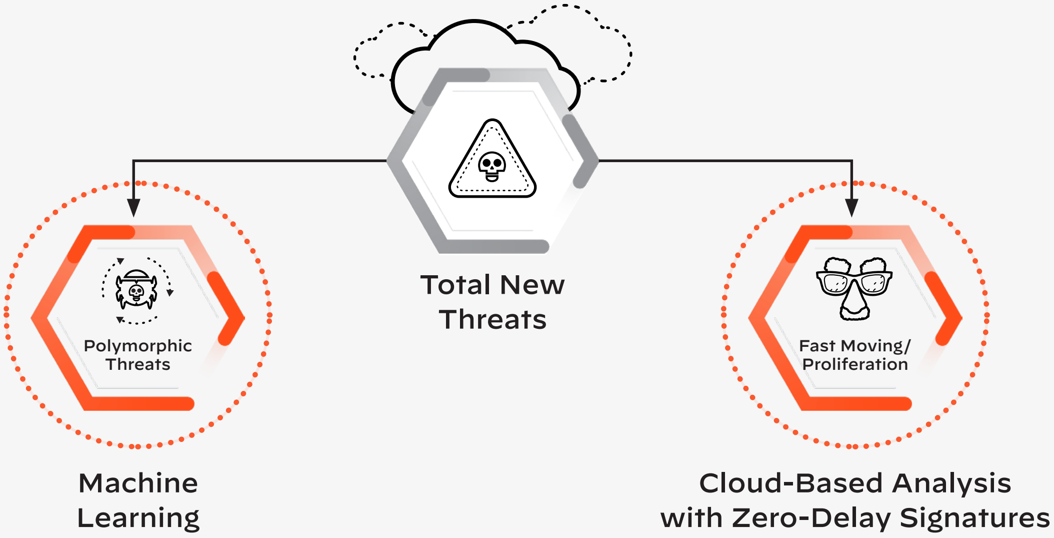
**Current Industry Response:** Security solutions typically attempt to crawl websites, either during or after the site has been visited, and add malicious sites to a database, which is then queried to protect subsequent visitors. This approach allows the initial attack to proceed, and at worst, by the time crawling occurs, the malicious site may not be available or could be cloaked.

**The ML-Powered NGFW Way:** Database lookup-based security will never keep up with the automated adversary. ML models are enabled directly on the NGFW, alerting on or stopping never-before-seen phishing and JavaScript attacks inline before they're unleashed on your organization. Malicious URLs are identified in milliseconds, with malicious JavaScript blocked instantly. If a URL is not deemed malicious, it is passed on to the URL Filtering cloud for detailed crawling analysis to determine its proper categorization and deliver a verdict within minutes.

## Zero-Delay Signatures Leveraging Massive Cloud Scale

**Challenge:** Even as inline ML in the NGFW delivers instant protection against new, never-before-seen malware variants, there remains a critical need to detect sophisticated and complex threats. As such, there are situations where accurate and timely signatures are essential for malware prevention. For example, nation-state-level attacks, as well as most sophisticated threat actor groups, will at times develop new malware completely from scratch—and security systems may have just seconds to respond to these threats. There are also file formats not covered by current ML-based models. Thus, to mitigate attacks of this nature, malware payloads must be analyzed in a robust, scalable cloud environment. Multiple detection techniques must be brought to bear in order to identify the malicious behavior, build new models, and map the indicators of compromise. That can take too long with a standard approach to signatures, analysis, and periodic update to the control points for enforcement.

Inline ML and Zero-Delay Signatures—Essential Tools to Combat Today's Malware



**What an ML-Powered NGFW Does:** To meet the challenges of new and evolving malware, it's critical to pair inline protection with real-time intelligence from the cloud. An ML-Powered NGFW reimagines and rearchitects the way signatures are delivered, once analysis is complete and models have been updated. Instead of having to wait a minimum of five minutes for a scheduled push, signature updates are now delivered and streamed to the connected ML-Powered NGFW within seconds, as soon as the inline ML-basis analysis is complete.

With zero-delay signatures, every single internet-connected NGFW in a network is updated within single-digit seconds of the analysis, ensuring the first user to see a brand-new threat is the only user to see the threat and future mutations are automatically prevented.

### Scenario: Targeted Zero-Day File-Based Attack

**Situation:** A threat actor deploys a customized or targeted threat designed to evade traditional malware sandboxes and antivirus products.

**Current Industry Response:** Traditional on-premises and cloud-based sandboxes use legacy-based approaches for blocking malware based on static information or attempt to delay the file to allow for analysis. This leads to false negatives, and more importantly, poor user experience. Hourly or longer periodic updates are not uncommon.

**The ML-Powered NGFW Way:** For novel, never-before-seen threats, an ML-powered NGFW leverages sophisticated, multi-technique, cloud-delivered ML models to identify and block malicious content with no user impact. Additionally, malware blocked in real time by the ML model is forwarded for full cloud-based analysis.

## ML-Powered Visibility Across IoT and Other Devices

**Challenge:** By 2021, it's estimated that 35 billion IoT devices will be installed worldwide.[1] Furthermore, according to Forrester Research, 45 percent of enterprises had some level of IoT deployment in mid-2020, with 26 percent of clients planning IoT deployment within the next 12 months. With the proliferation of IoT devices across the enterprise, there is an ever-growing need to leverage vast amounts of data and computing power to constantly analyze and detect attacks, and reprogram security infrastructure.

Without IoT security, enterprises are simply blind to a vast and growing number of devices on the network—most of which run unpatched open source software, and are connected to critical systems or are critical systems—and have very few security controls. To keep a network fully protected, every new IoT device added needs to be manually monitored, and network security must be updated with that device's fingerprint. During the time it takes to identify devices and make updates to the network, an organization is at risk.

**35B**
is the estimate of IoT devices that will be installed worldwide by 2021[1]

**45%**
of enterprises had some level of IoT deployment, in mid-2020

**26%**
of clients planning IoT deployment within the next 12 months

> ***"The first challenge organizations face when deploying IoT is visibility."***
>
> – **Stephanie Balaouras**
> VP & Research Director for Security, Forrester

[1] The IoT Rundown for 2020: Stats, Risks, and Solutions," Security Today, https://securitytoday.com/articles/2020/01/13/the-iot-rundown-for-2020.aspx.

**What an ML-Powered NGFW Does:** Instead of signatures, an ML-Powered NGFW uses ML to identify and classify all IoT and OT devices in an enterprise network, including those never seen before. An ML-Powered NGFW must work in concert with other IoT security technologies to quickly and accurately profile any IoT, OT, or IT device to reveal its type, vendor, model, firmware, and more. Bypassing the limitations of signature-based solutions in new device discovery, an ML-Powered NGFW can use cloud scale to compare device usage, validate profiles, and fine-tune models so devices don't go unmanaged.

### Scenario: Unmanaged IoT Device on Network Exhibiting Suspicious Behavior

**Situation:** A security camera in a pool of devices begins transmitting an image or a video clip via FTP to another system.

**Current Industry Response:** Reactive, signature-based IoT security solutions depend on prior knowledge or a pre-existing definition of the device to get visibility. Worse, there would be no ability to track anomalous or unexpected behavior.

**The ML-Powered NGFW Way:** By continually monitoring traffic and behavior from IoT devices, the ML-Powered NGFW automatically groups similar types of devices, such as tablets, cameras, and printers, leveraging ML-based classifications to deliver rapid visibility. From there, 0anomalous activity that strays from the baseline behavior is easily tracked.

## Automated, Intelligent Policy Recommendations

**Challenge:** The rate of change of the network, of applications, of devices, and of attacks is simply far faster than security administrators can keep up with using manual tools. Often, the fall back is to resort to overly permissive policies to avoid breaking applications. However, this opens up the network to a host of threats. The best approach would be to heavily leverage context as the foundation of security policy, coupled with constantly updated and automated industry best practices.

**The diversity involved in the IoT landscape makes policy decisions cumbersome:**

Diversity of hardware

Diversity of software

Diversity of operating systems

Diversity of protocols

**What an ML-Powered NGFW Does:** An ML-Powered NGFW  uses ML to analyze vast amounts of telemetry data and then automatically recommend security policies based on everything it sees across an organization's network. An ML-Powered NGFW enables administrators to confidently apply policy changes to reduce risk from IoT devices. By comparing metadata across millions of IoT devices with those found in the network, an ML-Powered NGFW can use device profiles to determine normal behavior patterns. For each IoT device and category of devices, it can then provide a recommended policy to restrict or allow trusted behaviors. Recommended policies can save countless hours per device in gathering the application usage, connection, and port/protocol data needed to create policies manually. Once reviewed, a policy can be quickly imported by a ML-Powered NGFW, with any changes automatically updated, keeping administration overhead to a minimum.

### Scenario: Misconfigured IoT Device Presents Security Risk

**Situation:** An IoT device that was improperly configured needs to be locked down.

**Current Industry Response:** In addition to visibility gaps, policy crafting can be challenging, often requiring manual pairing of IP addresses and devices.

**The ML-Powered NGFW Way:** Based on risk thresholds, alerts are generated, automatically recommending a tight Zero Trust policy to secure the device. The policies can easily be added to groups, and customers can adjust the policy to meet their needs

## The Benefits of an ML-Powered NGFW

The evolving and maturing security market continues to respond to the ever-changing threat landscape and shifting nature of attacker tactics. Now, more than ever, disrupting the status quo in network security is a necessity.  Attackers are successfully wielding distinct advantages, which include automation, cloud scale, and machine-driven assistance. For defenders, rather than simply responding, as has been the case historically with incremental measures, these same drivers provide a path to substantially change the game. At the core, the response involves an evolutionary progression to what has become the essential control point in the enterprise, the next-generation firewall, which was itself a complete disruption of the network security over a decade ago.

**With a ML-Powered NGFW, organizations can:**

Proactively prevent up to 95% of new threats instantly, blocking the initial infection inline and eliminating the potential spread.

Stop weaponized files, and malicious scripts without sacrificing the user experience.

Extend visibility and security to all devices on the network, including unmanaged IoT devices, without requiring additional sensors.

Automate policy recommendations to help save time, reduce the chance of human error, and prevent the most advanced attack methods.

How is Palo Alto Networks leveraging ML to protect enterprises from tomorrow's threats? Our ML-Powered NGFWs use ML to instantly prevent up to 95% of never-before-seen file and JavaScript threats inline. Our firewalls detect three times more IoT devices and utilize ML to create a less than ten-second signature delivery, resulting in a 99.5% reduction in systems infected. ML is helping us create a safer, more secure environment for our partners and customers.

Ready to test-drive our ML-Powered NGFWs?

**Click here and take an Ultimate Test Drive**

## About Palo Alto Networks

Palo Alto Networks, the global cybersecurity leader, is shaping the cloud-centric future with technology that is transforming the way people and organizations operate. Our mission is to be the cybersecurity partner of choice, protecting our digital way of life. We help address the world's greatest security challenges with continuous innovation that seizes the latest breakthroughs in artificial intelligence, analytics, automation, and orchestration. By delivering an integrated platform and empowering a growing ecosystem of partners, we are at the forefront of protecting tens of thousands of organizations across clouds, networks, and mobile devices. Our vision is a world where each day is safer and more secure than the one before. For more information, visit **www.paloaltonetworks.com**.